REMARKS

This Application has been carefully reviewed in light of the Office Action mailed May 22, 2003. Applicant appreciates the Examiner's consideration of the Application. Claims 14-20 have been added and Claims 1, 7, and 13 have been amended to clarify, more particularly point out, and more distinctly claim inventive concepts previously present in these claims. Applicant respectfully submits that no new matter has been added by the amendments to the specification or by the amendments to the claims. In order to advance prosecution of this Application, Applicant has responded to each notation by the Examiner. Applicant respectfully requests reconsideration and favorable action in this case.

Information Disclosure Statement

The Examiner calls to the Applicant's attention informalities in the Information Disclosure Statement filed on October 8, 1999. Applicant appreciates the Examiner's observation regarding the missing date entries. Accordingly, Applicant has re-submitted form PTO-1449 with the missing dates included.

Section 102 Rejection

The Examiner rejects Claims 1-5, and 7-13 under 35 U.S.C. § 102(e) as being unpatentable over U.S. Patent No. 5,319,776 issued to Hile et al. (*Hile*). Applicant respectfully submits that *Hile* fails to disclose, teach, or suggest the combination of limitations specifically recited in Applicants' claims.

For example, *Hile* fails to disclose, teach, or suggest:

(1) receiving "an input stream" at a binary state machine "prior to being buffered at a first network device, the input stream comprising a plurality of characters transmitted by a second network device";

(2) storing "a copy of the input stream" at a network interface disposed between the first network device and the second network device;

(3) discarding the first character "before selecting a next character of the input stream"; and

(3) transmitting "the copy of the input stream" to the first network device "if an attack on the computer network is not detected" (recited in Applicant's Claims 1, 7, 13-14, and 20).

First, *Hile* fails to disclose, teach or suggest receiving "an input stream" at a binary state machine "prior to being buffered at a first network device, the input stream comprising a plurality of characters transmitted by a second network device." *Hile* is directed to testing data in transit "between a source medium and a destination medium, such as between two computer[s] communicating over a telecommunications link or network." (*Hile*, Abstract). In particular, *Hile* states, "Referring to FIG. 1A, first computer system 12 and a second computer system 14 are diagrammatically illustrated. Each computer system has a bus 16, a central processing unit (CPU) 18a and 18b, respectively, random access memory (RAM) 20 and serial port 22." (*Hile*, column 3, lines 18-22). *Hile* further states that, "CPU 18b and RAM 20 associated with CPU 18b perform the in transit detection illustrated in the flow diagram of FIG. 1B. The input data stream over telecommunication link 26 enters the modem and serial port of computer system 14 where it is placed by CPU 18b into an input buffer 30 comprising a portion of RAM 20." (*Hile*, column 3, lines 61-67). That is, *Hile* discloses an incoming stream received at an input buffer at the second computer system 14, where the in transit detection is performed. This is even more evident from *Hile*'s Figure 1A, which shows that prior to reaching *Hile*'s finite state machine 32, the input data is buffered at buffer 30 associated with RAM 20 of the destination medium. Therefore, *Hile* does not disclose, teach, or suggest, receiving "an input stream" at a binary state machine "prior to being buffered at a first network device", as recited in Applicant's independent Claims 1, 7, 13-14, and 20.

Second, *Hile* fails to disclose, teach, or suggest storing "a copy of the input stream" at a network interface disposed between the first network device and the second network device", and transmitting "the copy of the input stream" to the first network device "if an attack on the computer network is not detected", as recited by Applicant's independent Claims 1, 7, 13-14, and 20. *Hile* states, "Typically, the input buffer 30 is configured to hold one or more blocks of data which have been transmitted over communication link 26 by the computer system 12." (*Hile*, column 3, lines 67-68; column 4, lines 1-2). *Hile* continues:

> When the incoming data stream has been error checked and the input buffer becomes filled, in a conventional data communications system, the data in buffer 30 would be stored on the destination medium 24b. The present invention intervenes at this point by subjecting the buffered data to a character by character virus signature string search analysis depicted at 32. The string search routine is preferably implemented using a finite state machine based on preloaded finite state table 34. If a virus signature is detected by the string search routing, the user is alerted at step 36, typically by an appropriate warning message displayed on the computer system monitor. Upon detection of a virus signature, any storage of the data onto destination medium 24b is terminated, with the receiving file being dealocated or marked to be overwritten.
>
> If no virus signature is detected, the data is stored on destination medium 24b as depicted at 38 and 40. Most computer operating systems buffer data being written to the storage medium. This buffer is illustrated at 38.

(*Hile*, column 4, lines 7-26). That is *Hile* buffers an incoming stream at the destination computer, performs a string search on the buffered incoming stream, and, if a virus is detected, the data of the incoming stream is dealocated or marked for deletion. If *Hile* does not detect a virus, the data of the incoming stream, already buffered at the destination computer, is further stored at 38 and 40 according to typical hard drive storage operations. Therefore, and for at least the above mentioned reasons, *Hile* does not disclose, teach, or suggest storing "a copy of the input stream" at a network interface disposed between the first network device and the second network device"; and transmitting "the copy of the input stream" to the first network device "if an attack on the computer network is not detected", as recited by Applicant's Claims 1, 7, and 13 as amended and Claims 14 and 20 as drafted. Consequently, Applicant respectfully requests that the Examiner withdraws the rejection to these Claims.

Additionally, *Hile* fails to disclose, teach, or suggest discarding the first character "before selecting a next character of the input stream" recited in Applicant's Claims 1, 7, 13-14, and 20. As already discussed, *Hile* buffers an incoming stream, performs a string search on the buffered incoming stream, and, if a virus is detected, the data of the incoming stream is dealocated or marked for deletion. If *Hile* does not detect a virus, the data of the incoming stream is further stored at 38 and 40 according to typical hard drive storage operations. Nothing in *Hile*, either expressly or impliedly, can be characterized as disclosing discarding the first character before selecting a next character of the input stream. In fact, *Hile*'s only

memory release occurs after a virus is detected at step 78 of *Hile*'s Figure 6C, where the routine "StrSrchStopSrch" is called to "Release Memory Used To Conduct Search." (*Hile*, Figure 6C). That is, only after a virus string has been detected, *Hile* releases memory, and then *Hile* only releases "the memory used by the virus string search routine", (*Hile*, column 7, lines 20-23), but does not discard a first character before selecting the next character of the input steam. Therefore, *Hile* does not disclose, teach, or suggest discarding the first character "before selecting a next character of the input stream", as recited in Applicant's independent Claims.

Moreover, neither would it be obvious for *Hile* to discard the first character "before selecting a next character of the input stream", because *Hile* would not work as intended. *Hile*'s input data stream is buffered at buffer 30, wherein resides the only copy of the data received. If *Hile* were to drop characters in the stream as the new state is generated, *Hile* would not be able to store the received data once the virus detection has been performed. As already discussed, *Hile* uses buffer 30 to store the input stream on which the virus string search is performed. Thereafter, "If a virus was detected during the transfer, the routine at step 78 can be made to purge the data in the file by overwriting it with 1's or 0's and the file is then deleted from storage." (*Hile*, column 7, lines 24-27). However, if no virus is detected, the data is unloaded from the buffer and stored in a file in the hard drive. (*Hile*, Fig 6B). If *Hile* were to drop each character from the buffer before selecting the next character in the input stream, at the end of the string search *Hile*'s buffer 30 would be empty, which, if no virus is detected, would leave an empty file in the hard drive that is supposed to include the checked input data. Therefore, *Hile* does not disclose, teach, or suggest the first character "before selecting a next character of the input stream", as recited in Applicant's independent Claims 1, 7, and 13 as amended and Claims 14 and 20 as drafted. Consequently, and for at least these reasons, *Hile*, fails to disclose, teach, or suggest the combination of limitations specifically recited in Applicants' independent Claims 1, 7, and 13-14, and 20.

Applicant's dependent Claims 2-6, 6-12, and 15-19 are allowable based on their dependence on the independent claims and further because they recite numerous additional patentable distinctions over the prior art. Because Applicant believes he has amply demonstrated the allowability of the independent claims over the prior art, and to avoid burdening the record, Applicant has not provided detailed remarks concerning these

dependent claims. Applicant, however, remains ready to provide such remarks if it becomes appropriate to do so.

Applicants therefore respectfully request reconsideration and allowance of independent Claims 1, 7, 13-14, and 20 and all claims that depend on these claims.

Section 103(a) Rejection

The Examiner rejected Claim 6 under 35 U.S.C. § 103(a) as being unpatentable over *Hile* in view of U.S. Patent No. 6,078,924 issued to Ainsbury et al. (*Ainsbury*). Applicant respectfully traverses this rejection for the reasons already discussed.

Therefore, and for at least the reasons provided, *Hile*, whether considered alone or in combination with any other prior art of record or with knowledge of one skilled in the art at the time of the invention, does not disclose, teach, or suggest the combination of limitations specifically recited in Applicant's independent Claims 1, 7, 13-14, and 20, and the claims the depend on these claims. Consequently, Applicant respectfully requests that the Examiner withdraw this rejection.

New Claims

New Claims 14-20 have been added and are fully supported by the original specification at page 7, lines 26-31; page 9, lines 3-14; and Figures 1-3. Applicants submit that no new matter has been added.

CONCLUSION

Applicant has made an earnest attempt to place this case in condition for allowance. For at least the foregoing reasons, Applicant respectfully requests full allowance of all the pending claims.

If the Examiner believes a telephone conference would advance prosecution of this case in any way, the Examiner is invited to contact Bradley P. Williams, the Attorney for Applicant, at the Examiner's convenience at (214) 953-6447.

Although Applicant believes no fees are due, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicant

Bradley P. Williams
Reg. No. 40,227

BPW/MLQ/ls

Correspondence Address:
Baker Botts L.L.P.
2001 Ross Avenue, Suite 600
Dallas, Texas 75201-2980
(214) 953-6447

Date: 7/9/03